

PCT

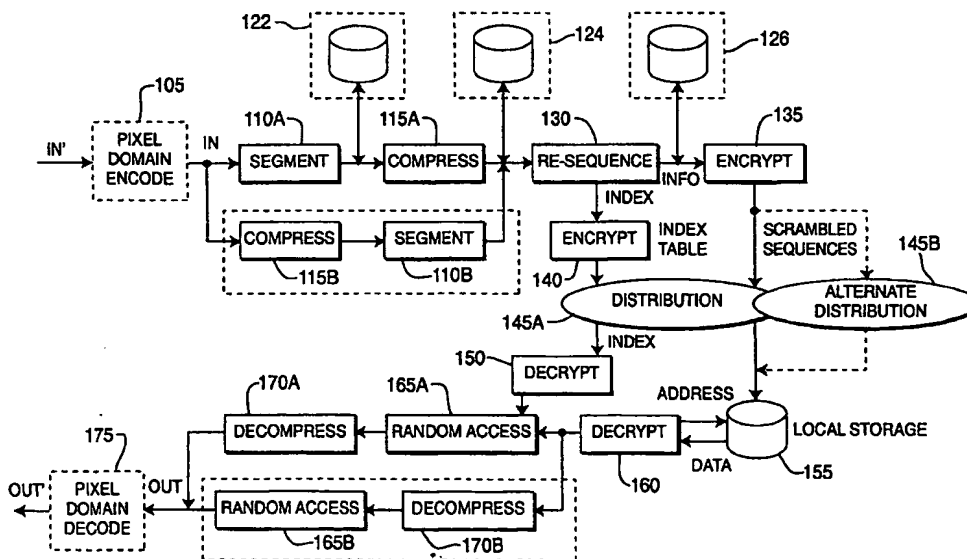
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167, H04L 9/06, H03M 7/30	A1	(11) International Publication Number: WO 00/11870 (43) International Publication Date: 2 March 2000 (02.03.00)
(21) International Application Number: PCT/US99/18417 (22) International Filing Date: 12 August 1999 (12.08.99) (30) Priority Data: 60/097,264 20 August 1998 (20.08.98) US 09/182,933 30 October 1998 (30.10.98) US (71) Applicant: SARNOFF CORPORATION [US/US]; 201 Washington Road, CN5300, Princeton, NJ 08543 (US). (72) Inventors: REITMEIER, Glenn, A.; 193 Cinnabar Lane, Yardley, PA 19067 (US). TINKER, Michael; 35 Highland Drive, Yardley, PA 19067 (US). (74) Agents: BURKE, William, J. et al.; Sarnoff Corporation, 201 Washington Road, CN5300, Princeton, NJ 08543 (US).		(81) Designated States: BR, CA, CN, IN, JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: SECURE INFORMATION DISTRIBUTION SYSTEM UTILIZING INFORMATION SEGMENT SCRAMBLING



(57) Abstract

A method and apparatus for securing and, optionally, distributing an information stream by dividing the information stream into a collection of segments and compressing the segments, rearranging the order of the segments and encrypting the segments.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Secure Information Distribution System Utilizing Information Segment Scrambling

This application claims the benefit of U.S. Provisional Application No.
5 60/097,264, filed August 20, 1998, which is herein incorporated by reference in its entirety.

The invention relates to information distribution systems and, more particularly, the invention relates to methods and apparatus for securing
10 information distributed within an information distribution system.

BACKGROUND OF THE DISCLOSURE

In several communications systems the data to be transmitted is compressed so that the available bandwidth is used more efficiently. For
15 example, the Moving Pictures Experts Group (MPEG) has promulgated several standards relating to digital data delivery systems. The first, known as MPEG-1 refers to ISO/IEC standards 11172 and is incorporated herein by reference. The second, known as MPEG-2, refers to ISO/IEC standards 13818 and is incorporated herein by reference. A compressed digital video system is described
20 in the Advanced Television Systems Committee (ATSC) digital television standard document A/53, and is incorporated herein by reference.

The above-referenced standards describe data processing and manipulation techniques that are well suited to the compression and delivery of video, audio and other information using fixed or variable length digital
25 communications systems. In particular, the above-referenced standards, and other "MPEG-like" standards and techniques, compress, illustratively, video information using intra-frame coding techniques (such as run-length coding, Huffman coding and the like) and inter-frame coding techniques (such as forward and backward predictive coding, motion compensation and the like).
30 Specifically, in the case of video processing systems, MPEG and MPEG-like video processing systems are characterized by prediction-based compression

encoding of video frames with or without intra- and/or inter-frame motion compensation encoding.

Present electronic distribution systems typically do not strike an appropriate balance between flexibility and security for the purposes of some information distribution applications. For example, to enable the electronic distribution of motion pictures (i.e., film) and other entertainment video applications, it is necessary to dynamically process "trailers" (i.e., short previews of coming attractions") on a location by location basis, in addition to full length motion pictures. With respect to security, it is obviously necessary to incorporate a high level of security, ideally using a multi-layer security approach, such that the valuable intellectual property transmitted within the system is not compromised.

Therefore, a need exists in the art for a secure and flexible method and apparatus for distributing information such as high-value motion pictures and other audio-video information, as well as other forms of data. Additionally, it is seen to be desirable to provide enhanced security for various media, such as digital versatile disk (DVD) and other media.

SUMMARY OF THE INVENTION

A method and apparatus for securing and, optionally, distributing an information stream by divided the information stream into a collection of segments and compressing the segments, rearranging the order of the segments and encrypting the segments prior to, e.g., distributing the encrypted segments to one or more users within an information distribution system.

Specifically, in one embodiment of the invention, an input information stream is divided into a collection of information segments, the individual segments are then compressed and arranged in a non-standard (i.e., scrambled) manner to produce a scrambled collection of information segments and an associated index table suitable for use in rearranging the collection of information segments into a standard (i.e., unscrambled) order. The scrambled collection of information segments and the associated index table are encrypted (using the same or different encryption techniques) and distributed to one or

more subscribers (using the same or different distribution channels). Optionally, the scrambled collection of information segments is distributed using a plurality of distribution channels (i.e., multipath distribution) and/or at a plurality of different times (i.e., temporally staggered distribution).

5

BRIEF DESCRIPTION OF THE DRAWING

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

10 FIG. 1 depicts an information distribution system 100 including apparatus according to the invention;

FIG. 2 depicts a graphic representation of collection of information segments arranged in a non-standard (i.e., scrambled) order, and an index table suitable for use in rearranging the collection of information segments into a

15 standard (i.e., unscrambled) order;

FIG. 3 depicts a flow routine of an information provider processing method according to the invention;

FIG. 4 depicts a flow diagram of a subscriber side method for processing an information stream according to the invention; and

20 FIG. 5 depicts a diagrammatic representation of the a layered security environment enabled by the invention.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

25

DETAILED DESCRIPTION

The invention will be described within the context of an MPEG-like information distribution system. It will be recognized by those skilled in the art that the invention is applicable to many types of information distribution systems. More specifically, the invention is ideally suited to the protection and
30 dissemination of information streams comprising related sequenced of video and/or audio information, such as motion pictures, television and the like.

FIG. 1 depicts an information distribution system 100 including apparatus according to the invention. Specifically, FIG. 1 depicts an information distribution system 100 comprising information provider equipment (105-140), information distribution channels (145A and 145B), and subscriber equipment 5 (150-175). The information distribution system 100 receives an input information stream IN', illustratively an audio-visual information stream such as a motion picture video stream and one or more associated audio or data streams. The input information stream IN' is processed by the provider equipment to produce a secure information stream that is coupled to the 10 subscriber equipment via the information distribution channel(s). The secure information stream is received and processed by the subscriber equipment to produce an output information stream OUT' comprising the initial audio-visual information stream IN'.

In one embodiment of the invention, a movie or other program is 15 compressed as a collection of self-contained MPEG-2 sequences, which may be of non-uniform duration and size (number of bits). For distribution/storage, the sequences may be arbitrarily re-ordered and an index table built that contains pointers to the storage locations of sequences ordered in their correct presentation sequence. The reordered sequences may be encrypted using 20 standard encryption techniques. The index table may be separately encrypted using the same or different encryption techniques. In addition, the index table may be distributed using a different medium. For example, the encrypted and re-ordered sequences may be distributed on a DVD-ROM, while the encrypted index table is downloaded to the receiver/decoder from an on-line server.

25 Alternatively, a smart card could be used for the index table. Many variations are possible. At the receiver, the decrypted index table is used to control the random access readout of the encrypted sequences from the storage medium. The video sequences are decrypted, decompressed and displayed in their proper order.

30 The index table approach not only achieves scrambling, but it also provides an approach to flexibly accommodate trailers. The re-ordered video storage distributed to all locations would contain all trailers. The index table

distributed to a particular location may indicate the desired subset of trailers. In this manner, the index table and reordering approach provides both multi-level security and trailer-handling flexibility.

It should be noted that within the scope of this invention, video and audio
5 may be separately segmented and independently re-ordered, with separate index tables for each. Similarly, separate video components (e.g., R, G and B) may also be treated separately.

The information provider equipment within the information distribution system 100 of FIG. 1 comprises an optional pixel domain encoder module 105, a
10 segmentation module 110, a compression module 115, a re-sequencing module 130, an information stream encryption module 135, an index table encryption module 140, and a plurality of optional provider storage modules 122, 124 and 126.

The optional pixel domain encoder 105 receives and processes the input
15 information stream IN' according to one or more of a plurality of pixel domain (or audio domain) processing techniques. These techniques will be described in more detail below with respect to FIG. 3. As an example, the optional pixel domain encoder 105 may impart a digital watermarking to video information within the received input information stream IN' such that copyright notices,
20 source designation and other information related to, e.g., the allowable use and/or ownership of the input information stream IN' may be inserted. The pixel domain encoder 105 produces a pixel (or audio) domain encoded information stream IN that is coupled to the segmentation module 110. It should be noted that within the context of this disclosure, the term "pixel domain" is used to
25 denote more than the pixel or baseband video or image information. The term "pixel domain" is used to additionally denote audio and other information (i.e., data) associated with the pixel or baseband video or image information of the underlying information stream being processed.

The segmentation module 110 divides the encoded (or unencoded)
30 information stream IN into a plurality of segments to produce a segmented information stream. The segmented information stream is then coupled to compression 115A and, optionally, stored in a first provider storage module 122.

That is, the segmentation module 110 "chops" the input information stream IN into a plurality of information segments of the same or different lengths according to one or more of a plurality of criteria. The criteria will be described in more detail below with respect to FIG. 3.

5 In one embodiment of the invention, the segmentation module 110 may arbitrarily "chop" the input information stream IN into segments of, e.g., 1000 packets up to an appropriate stream splicing exit point. In another embodiment of the invention, the segmentation module 110 delineates a predefined, approximate number of frames (e.g., approximately 100 or 1000 frames) within a
10 video stream. The selected segment of frames includes those frames immediately preceding a scene cut (e.g., those frame immediately preceding an I-frame). In still another embodiment of the invention, the segmentation module 110 an approximate number of video frames and associated audio frames are selected such that the segment thereby formed includes all the audio frames
15 associated with the video segment (i.e., no audio frames in one segment that are related to video frames in another segment).

 It is desirable to avoid leaving "clues" to the scrambling process, such that a hacker might be able to piece together the various segments. For example, audio frames having known associations to video frames may be used to
20 reconstruct the appropriate arrangement of the video frames. That is, discontinuities within the audio track (i.e., a break within the middle of a musical note or tone) may be matched together to reconstruct a video segment. Therefore, in one embodiment of the invention the audio frames are segmented separately from the video frames.

25 The segment size is determined with respect to the security level desired (i.e., more or smaller segments yields greater security), the structure of the underlying information (i.e., fixed or variable group of pictures, frequent video scene cuts and the like).

 The compression module 115A compresses the segmented information
30 stream according to, e.g., an MPEG or other compression scheme, depending upon the type of information being distributed. For example, in the case of the input information stream in comprising a video information stream and

associated audio information stream (e.g., a motion picture), compression module 115A may be used to encode the video information according to an MPEG-2 compression technique, and the audio information according to an AC-3 or other audio encoding technique. Compression module 115A produces a compressed
5 information stream that is coupled to re-sequencing module 130 and, optionally, stored in a second provider storage module 124.

It should be noted that the order of segmentation module 110A and the compression module 115A may be reversed. Thus, in FIG. 1, an alternate processing path for the input information stream IN is provided in which a
10 compression module 115B is used to process the input information stream IN prior to segmentation by a segmentation module 110B.

Re-sequencing module 130 rearranges the compressed information segments according to a predetermined or pseudo-random pattern. That is, re-sequencing module 130 "shuffles" the compressed and segmented information
15 stream to produce a reordered or re-sequenced compressed and segmented information stream and an associated index table indicative of the re-sequencing operation performed upon the compressed and segmented information stream. The re-sequencing module 130 re-sequences the underlying video and/or audio information according to one or more of several criteria, such as scene
20 boundaries, GOP size, temporal or frame displacements, frame count, and the like. The re-sequenced compressed and segmented information stream is coupled to the information stream encryption module 135, while the associated index table is coupled to the index table encryption module 140. Optionally, the output of re-sequencing module 130 is coupled to third local storage module 126.

25 It is critical to the understanding of the present invention to note that the purpose of the segmentation module 110A and the re-sequencing module 115A is to rearrange, in a seemingly random manner, e.g., the video and/or audio information associated with an underlying audio-video information stream such that the presentation continuity of the underlying audio-video information is
30 destroyed. That is, the segmentation module 110A and the re-sequencing module 115A remove the temporal continuity of the underlying audio video

information in a manner that renders the audio-video information unusable, or at least unenjoyable, to a pirate or unauthorized subscriber.

The information stream encryption module 135 scrambles the re-sequenced compressed and segmented information stream using one or more
5 known scrambling techniques. Additionally, the index table produced by re-sequencing module 130 is coupled to another encryption module 140, where it is encrypted in one of a number of known manners to produce an encrypted index table. The encrypted information stream (i.e., the scrambled re-sequenced, compressed and segmented information stream) and the encrypted index table
10 are coupled to information consumer or subscriber side equipment via, e.g., distribution network 145 and/or alternate distribution network 145A.

The optional first 122, second 124 and third 126 local storage module 126 are used to store, respectively, the output of segmentation module 110A (or compression module 115B), the output of compression module 115A (or
15 segmentation module 110B) and the output of re-sequencing module 130. The local storage modules may be used to, e.g., store such information for further processing by additional processing devices (not shown) or to allow processing of an entire information stream at each step (e.g., perform all segmentation of a received input information stream IN, then perform all compression of the
20 segmented information stream, then perform all re-sequencing of the compressed and segmented information stream, etc.). Optionally, the server side equipment may be used as a temporary buffer during a "one pass" processing of an input information stream IN (such as a live broadcast of a baseball game).

Distribution network 145A and alternate distribution network 145B may
25 comprise any one of a number of standard distribution networks such as, microwave links, fiber optic networks, satellite links, cable television links, DVD, Internet, broadcast and the like.

In one embodiment of the invention an alternate distribution network 145B is utilized to transport some of all of the scrambled sequences produced by
30 encryption module 135. That is, the alternate distribution network 145B may be used to transport, e.g., every fifth or some other portion of the scrambled sequences produced by the encryption module 135. In this manner, an

unauthorized user intercepting the information carried by distribution network 145A would, even in the case of breaking the various encrypt codes and properly re-sequencing the scrambled segments, be unable to retrieve all of the scrambled sequences. Thus, alternate distribution network 145B provides an additional

5 layer of security within the information distribution system 100 of FIG. 1.

The subscriber side equipment within the information distribution system 100 of FIG. 1 comprises a local storage module 155, a decryption module 150, a second decryption module 160, a random access module 165, a decompression module 170 and an optional pixel domain decoding module 175.

10 The local storage module 155 receives the scrambled sequences transported by distribution network 145A and/or 145B and stores the scrambled sequences. The first decryption module 150 is used to decrypt the encrypted index table transported by distribution network 145A to produce a decrypted index table. The decrypted index table is coupled to random access module 165.

15 Second decryption module 160 accesses local storage module 155 to retrieve scrambled sequences that are stored and, responsively, decrypt those scrambled sequences. The decrypted scrambled sequences (i.e., unscrambled sequences) are then coupled to random access module 165. Random access module 165 utilizes the index table information received from first decryption module 150 to

20 rearrange the descrambled sequences received from decryption module 160 to produce a properly sequenced information stream at an output. That is, the output of random access module 165 comprises an information stream having a plurality of segments that are arranged in a manner providing continuity within the underlying, illustratively, audio visual information stream. Decompression

25 module 170 receives the information stream produced by random access module 165 comprising correctly arranged information segments and, responsively, decompresses the received information stream to produce one or more output information streams (i.e., an audio information stream, a video information stream and any ancillary data streams). The output information stream OUT is

30 optionally subjected to pixel domain decoding module 175, where a pixel domain decode process that is inverse of the pixel domain encoding process performed by pixel encoder 105 occurs.

FIG. 2 depicts a graphic representation of collection of information segments arranged in a non-standard (i.e., scrambled) order, and an index table suitable for use in rearranging the collection of information segments into a standard (i.e., unscrambled) order. In the graphic representation of FIG. 2, the collection of information segments are stored in a memory such as local storage unit 155 of the system 100 of FIG. 1, and the index table comprises a list of storage locations from which to read, in order, to reconstruct the original order of the information segments. In this manner, improperly obtained distributed data that is scrambled is not useful unless the index table is also obtained.

Specifically, FIG. 2 depicts an association between six locations (A-F) and six sequences (sequence 1 - sequence 6). It should be noted that in FIG. 2 an oval indicative of a storage module is shown containing a table associating the locations and sequences. Specifically, location A is associated with sequence 3, location B is associated with sequence 5, location C is associated with sequence 2, location D is associated with sequence 1, location E is associated with sequence 6 and location F is associated with sequence 4. Thus, an index table comprising the following sequence {D, C, A, F, B, E} indicates that the sequence is stored in memory should be retrieved, prior to being utilized, according to the associations described above to produce a properly sequenced information stream.

FIG. 3 depicts a flow routine of an information provider processing method according to the invention. The routine 300 depicted in FIG. 3 is directed towards processing an audio video stream to produce a segmented, encoded, re-sequenced and encrypted audio and video information stream and associated index information suitable for re-sequencing the segments.

The routine 300 is entered at step 302 and proceeds to step 304. At step 304 an optional pixel domain encoding process is performed on the video information within a received audio video information stream. For example, the pixel domain encoding process of step 304 may comprise a watermarking process, a pixel encryption process, a lip sync modification process, an audio suppression process or a chroma stripping process. Watermarking involves the insertion of identifying an issue within video portion of an information stream

such that copyright and other source indicative information may be included within a distributed information stream. Pixel encryption comprises any one of a number of encryption techniques which render pixel information unusable without the corresponding pixel decryption processing. Lip sync modification
5 comprises a change in synchronization of the video and associated audio information based upon a random or predetermined temporal parameter such that video and audio are no longer synchronized, thereby severely degrading the presentation of the audio video information stream. Audio suppression comprises techniques for suppressing or otherwise hiding audio information from
10 a downstream audio decoder, such that the audio information may only be retrieved by a decoder cognizant of the new location or encoding technique used to hide the audio information. Chroma stripping comprises a process for removing or hiding chrominance information from a downstream video decoder, such that the chrominance information may be retrieved only by decoder
15 cognizant of the location or technique used to hide the chrominance information. The routine 300 then proceeds to step 306.

At step 306 the audio video information stream is segmented into a plurality of contiguous information stream segments. These segments may be determined with respect to scene cut indicia, temporal displacement parameters,
20 frame counts, GOP structure and the like. The segments may be of the same or substantially the same length or the segments may be of variable lengths. Each segment is associated with a segment identifier such that the original segment arrangement may be preserved by storing segment identifiers with a stream index table. The routine 300 then proceeds to step 308.

25 At step 308 the segments are compressed according to, e.g., MPEG-2 video and related audio compression techniques. Since the stream segments produced at step 306 are typically self contained with respect to buffer behavior, the compression processes utilized at step 308 may be performed in parallel. That is, multiple audio visual stream segments may be compressed in parallel using a
30 parallel processing or parallel encoding technique. Otherwise, a single MPEG or other compression module may be used to process each stream segment in a standard manner to produce a compressed output stream comprising a plurality

of compressed stream segments. The routine 300 then proceeds to step 310. At step 310 the compressed stream segments are re-sequenced (i.e., "shuffled") to produce a re-sequenced compressed audio video information stream and associated index table. The index table includes information relating the re-sequenced segments to the initial sequence of segments such that the re-sequenced information stream segments may be rearranged to produce the initial stream segment order. The routine 300 then proceeds to step 312.

At step 312 each of the re-sequenced information stream segments are encrypted to produce an information stream comprising a plurality of encrypted, re-sequenced information stream segments. The routine 300 then proceeds to step 314, where the index table used to maintain inter-segment associations is itself encrypted. The routine 300 then proceeds to step 316. At step 316 the encrypted information stream segments and the encrypted index table are distributed via, e.g., an information distribution network. The routine 300 then proceeds to step 318 where it is exited.

FIG. 4 depicts a flow diagram of a subscriber side method for processing an information stream according to the invention. Specifically, the routine 400 of FIG. 4 is directed towards processing a received encrypted index table and encrypted information segments to extract a properly sequenced audio visual information stream for subsequent presentation. The routine 400 is entered at step 402 and proceeds to step 404.

At step 404 an encrypted index table received via a distribution network is decrypted to provide a usable index table. The routine 400 then proceeds to step 406, where a plurality of encrypted information stream segments are decrypted to produce decrypted information stream segments. It must be noted that the decrypted information stream segments are not in a correct sequence with respect to the underlying audio visual information. That is, the decrypted information segments are "shuffled" such that presentation of the encrypted information stream segments (after, of course, decompression) would result in an undesirable choppy, temporally discontinuous audio visual presentation. The routine 400 then proceeds to step 408.

At step 408 the decrypted information stream segments are accessed according to information within the decrypted index table. Specifically, the decrypted index table indicates a correct temporal order or sequence for the decrypted information stream segments. Decrypted information stream
5 segments are retrieved from, e.g., a local storage module in a correct temporal or sequential order as indicated by the decrypted index table to produce a properly sequenced compressed information stream. The routine 400 then proceeds to step 410, where the properly sequenced compressed information stream is decompressed to produce a decompressed audio visual information stream. For
10 example, the decompression process at step 410 is the inverse of the compression process used at step 308 of the routine 300 of FIG. 3. The routine 400 then proceeds to step 412.

At step 412 an optional pixel domain decoding process is used to decode any pixel domain encoding imparted to the information stream at step 304 of the
15 routine 300 of FIG. 3. The routine 400 then proceeds to step 414, where it is exited.

The above-described invention simultaneously provides for both flexibility and security of electronically stored video information. The essential observation is that, if compressed in an appropriate manner, video information
20 that is stored on a random access storage device can be re-sequenced with respect to its presentation flow. In normal operation, compressed video typically cannot be chopped up and stored in segments, because the use of bi-directional motion prediction and the constraints of neither overflowing nor underflowing rate buffers prohibit such operation. However, the MPEG-2 syntax does provide
25 mechanisms to treat portions of the video stream as self-contained entities. These mechanisms include the use of I and P frame GOP structures (e.g., "IPPPPPPI...") or other "closed" GOP structures (e.g., "IBBPBBPI...") and the use of splice point syntax that indicates periodic points at which buffers are filled to a known state. The invention provides an overall system that including both
30 flexibility and security.

It must be noted that if the segments are not self contained (e.g., not a closed GOP data structure), the VBV buffer status at the boundaries would

provide information to greatly assist in breaking the scrambling and reassembling of the proper video or audio sequence without the decrypted index.

It is important to note that the invention addresses the security weaknesses associated with continuity indicators, such as audio continuity, VBV
5 buffer status, PTS and DTS information and the like. These continuity indicators are useful to those seeking to break the security of the system and retrieve the "secured" data. By isolating or encapsulating such continuity indicators within a segment, and then encoding the segment, the continuity indicators are not useful in decoding the segment.

10

FIG. 5 depicts a diagrammatic representation of the a layered security environment enabled by the invention. Specifically, FIG. 5 depicts a series of concentric circles representative of security layers. The various layers of security have been described in detail above with respect to FIGS. 1-4. FIG. 5 is useful
15 in understanding the holistic, yet flexible approach to security that is enabled by the invention.

Specifically, a first layer of security is provided by a pixel domain or other baseband information domain (e.g., audio or data domain) processing layer
510. As previously discussed, the exemplary pixel domain process may comprise,
20 e.g., digital watermarking of video information, insertion of copyright notices and other pixel domain security measures. In the case of an information stream comprising an audio information stream or other information stream, the pixel domain process will, of course, comprise an audio domain process or other data domain process.

25 The security aspects of the pixel domain processing layer 510 are augmented by a stream segmentation processing layer 520. The security aspects of the stream segmentation processing layer 520 are augmented by a stream segment scrambling or re-sequencing layer 530. The security aspects of the stream segment scrambling or re-sequencing layer 530 are augmented by an
30 encryption layer 540, including an optional index encryption layer 535.

In addition to the above-described security layers 510-540, two additional optional security layers are provided. The first of the additional

optional layers comprises a multipath distribution layer 550, in which an information stream processed according to one or more of processing steps 510 through 540 is transmitted or distributed to one or more users via multiple signal paths. For example, the encrypted index produced at step 535 may be
5 transmitted via a different signal path or medium than the encrypted sequence of segmented or re-scrambled information frames produced at step 540.

The second of the additional optional layers comprises a temporal staggering layer 560, in which portions of the information stream processed according to one or more of processing steps 510 through 540 is transmitted to
10 one or more information consumers in a temporarily noncontiguous manner. That is, contiguous information stream segments are transmitted at different times (i.e., in temporally noncontiguous manner) and temporally reassembled by the information consumer(s).

In the case of a single transmission channel, the temporal staggering
15 security layer 560 cannot be used for real time distribution of secure information streams due to the inherent nature of temporal staggering (i.e., inherently not real time using a single channel). However, temporal staggering coupled with multipath distribution may be used to distribute real time information streams. For example, if three distinct communication channels are used to distribute
20 encrypted information segments, then each of the three channels may be used to distribute encrypted information segments offset by three segments from the information segment previously transmitted on that channel. From the perspective of a single channel, each of the transmitted information segments is temporally offset from a preceding or following information stream segment by
25 the time normally associated with transmitting the two intervening information stream segments (i.e., the time normally allocated to transmitting the two information stream segments carried by the other two channels is not used by the one channel). Optionally, this "dead time" may be filled with dummy information or information likely to cause errors or otherwise help thwart an
30 unauthorized user.

In one embodiment of the invention, one or more information distribution channels are used to transmit a plurality of segmented information streams. In

this embodiment of the invention, the information segments associated with each of the plurality of segmented information streams are interleaved across the one or more information to be transmitted are interleaved among one or more information distribution channels. The segmented information streams
5 may optionally share encryption keys. The interleave method may be fixed or dynamic. In the case of a dynamic interleave method, information suitable for reconstructing the various information streams may be provided within one or more index tables.

While the amount of security afforded by an individual security layer is
10 roughly represented by the relative position of the individual security layer, it must be noted that each layer addresses a different security threat. For example, the pixel domain (or, more generally, the baseband information domain) layer is addresses the identification and/or tracing of unauthorized information stream use and/or users. The segment scrambling and encryption
15 layers address the threat of hackers or other unauthorized users gaining access to useful data within a received information stream. The multiple channel transmission and temporal staggering layers address the physical avoidance of information stream reception by unauthorized users. The entire layered approach is directed toward providing selective layers of security, depending
20 upon, e.g., the sensitivity of the information to be distributed. For example, securing an electronic program guide may be deemed to be unnecessary. However, securing a first run movie distributed to theaters for subsequent presentation is absolutely necessary.

Although various embodiments which incorporate the teachings of the
25 present invention have been shown and described in detail herein, those skilled in the art can readily devise many other varied embodiments that still incorporate these teachings.

What is claimed is:

1. In an information processing system, a method for securing an
5 information stream comprising a sequence of information frames, said method comprising the steps of:
segmenting (306) said information stream into a plurality of information stream segments having a first segment sequence, each of said information stream segments comprising a plurality of information frames;
10 compressing (308) said information frames forming said information stream segments;
re-sequencing (310) said information stream segments to produce a re-sequenced information stream having a second segment sequence, said first segment sequence being related to said second segment sequence by an index;
15 and
encrypting (312, 314) said re-sequenced information stream and said index.
2. The method of claim 1, further comprising the steps of:
20 distributing (316) said encrypted re-sequenced information stream and said index to one or more information consumers.
3. The method of claim 2, wherein, said step of distributing comprises the steps of:
25 distributing, via a first medium (145A), said encrypted re-sequenced information stream; and
distributing, via a second medium (145B), said encrypted index.
4. The method of claim 2, wherein said encrypted and re-sequenced
30 information stream segments are distributed to said one or more information consumers in a temporally discontinuous manner.

5. The method of claim 4, wherein:

said second distribution channel comprises a plurality of distribution channels, each of said plurality of distribution channels distributing a respective plurality of said encrypted and re-sequenced information stream segments.

5

6. The method of claim 1, wherein:

a first compressed information frame within each of said information segments comprises a non-predicted information frame.

10 7. The method of claim 1, wherein:

said information stream comprises a plurality of image frames and associated audio frames; and

each of said information stream segments includes a respective first plurality of image frames and a respective second plurality of audio frames, said
15 first plurality of image frames and said second plurality of audio frames intended for presentation during substantially the same temporal period.

8. The method of claim 1, wherein said information stream comprises a plurality of image frames and associated audio frames, and wherein said step of
20 segmenting comprises the steps of:

segmenting said information stream into a plurality of image information stream segments having said first segment sequence, each of said image information stream segments comprising a plurality of image frames;

segmenting said information stream into a plurality of audio information
25 stream segments having a third segment sequence, each of said audio information stream segments comprising a plurality of image frames.

9. The method of claim 1, wherein

said step of compressing said information frames produces control
30 information indicative of a utilization level of a decoder buffer; and
said step of encrypting includes a step of encrypting said indicia of decoder buffer utilization.

10. In an information processing system, a method for recovering information frames from an information stream formed according to the securing method of claim 1, said method for recovering comprising the steps of:

5 recovering (404) said index relating said second segment sequence to said first segment sequence;

decrypting (406) said encrypted information stream segments to produce corresponding decrypted information stream segments;

re-sequencing (408), using said recovered index, said decrypted
10 information stream segments; and
decompressing (410), using a decompression process associated with said compression process, said compressed information frames included within said decrypted information stream segments.

15 11. The method of claim 10, wherein said step of re-sequencing comprises the steps of:

accessing, from a random access storage containing at least some of said decrypted information stream segments, said decrypted information stream segments according to said first segment sequence.

20

12. In an information processing system, apparatus comprising:

a segmentation module (110), for segmenting an information stream into a plurality of information stream segments, said information stream segments arranged according to a first segment sequence, each of said information stream

25 segments comprising a plurality of information frames;

a compression module (115), for compressing said information frames forming said information stream segments;

a re-sequencing module (130), for re-arranging according to a second segment sequence, said information stream segments including said compressed
30 information frames, said first segment sequence being related to said second segment sequence by an index; and

an encryption module (135), for encrypting said re-sequenced information stream segments and said index.

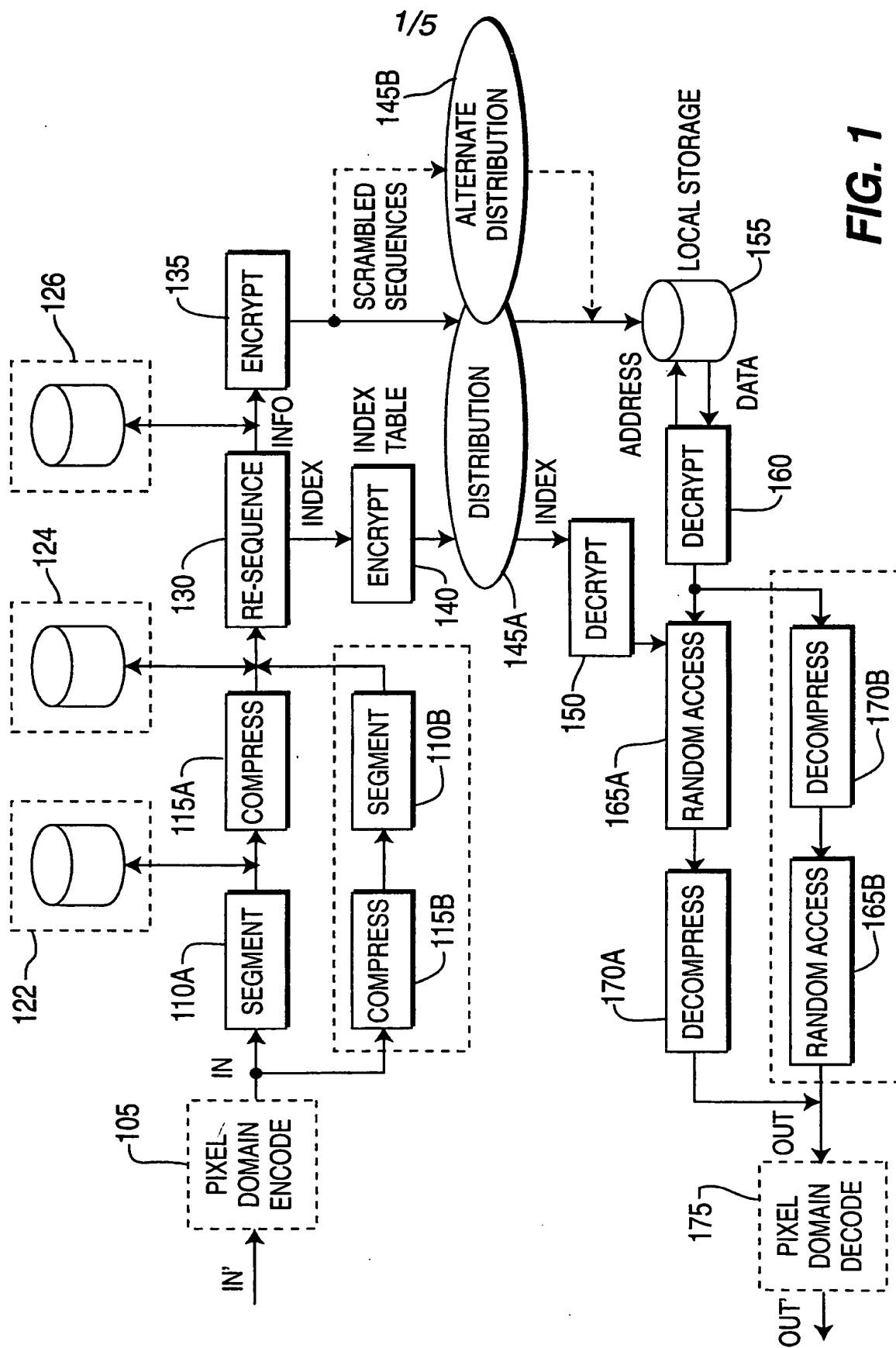


FIG. 1

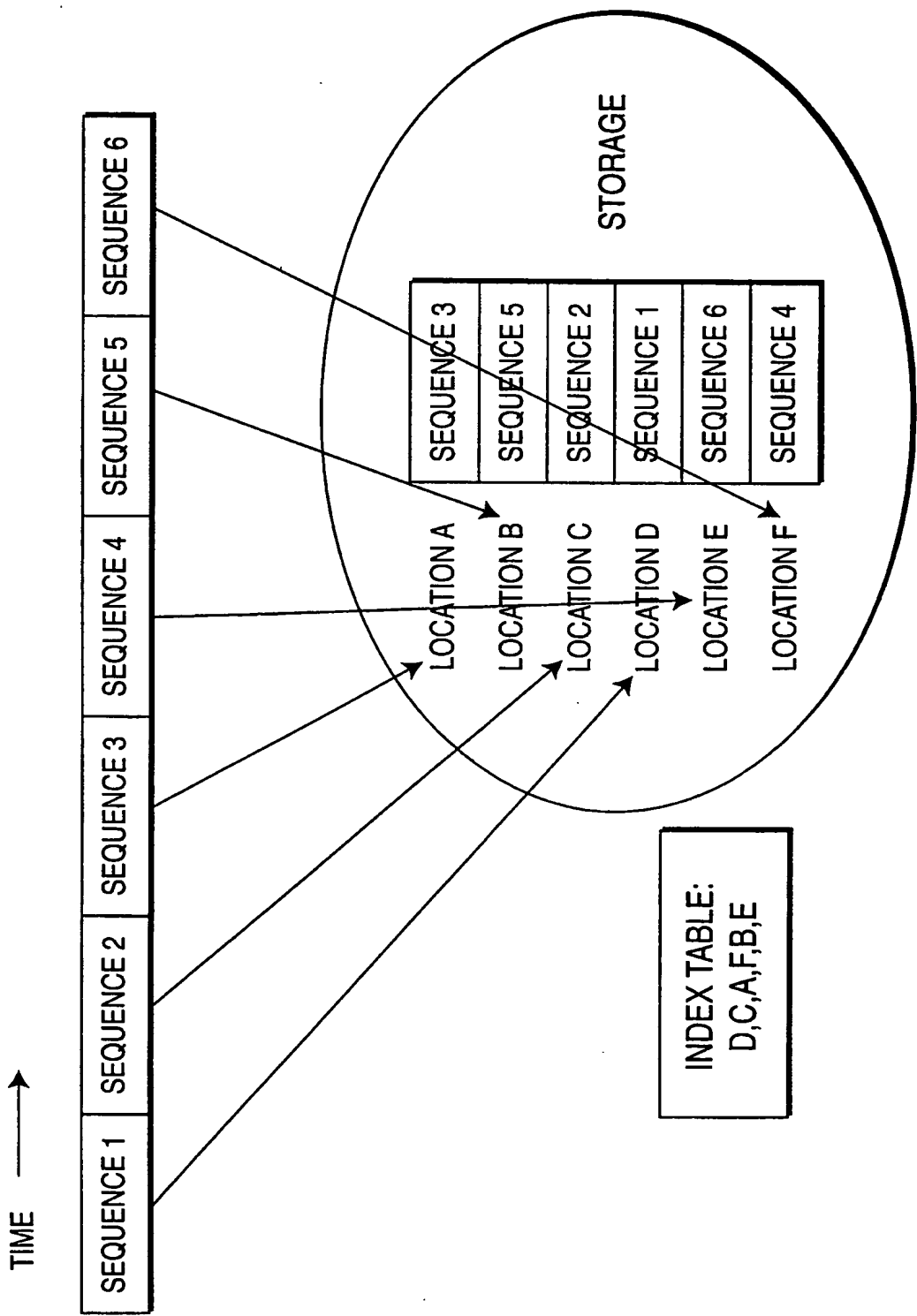
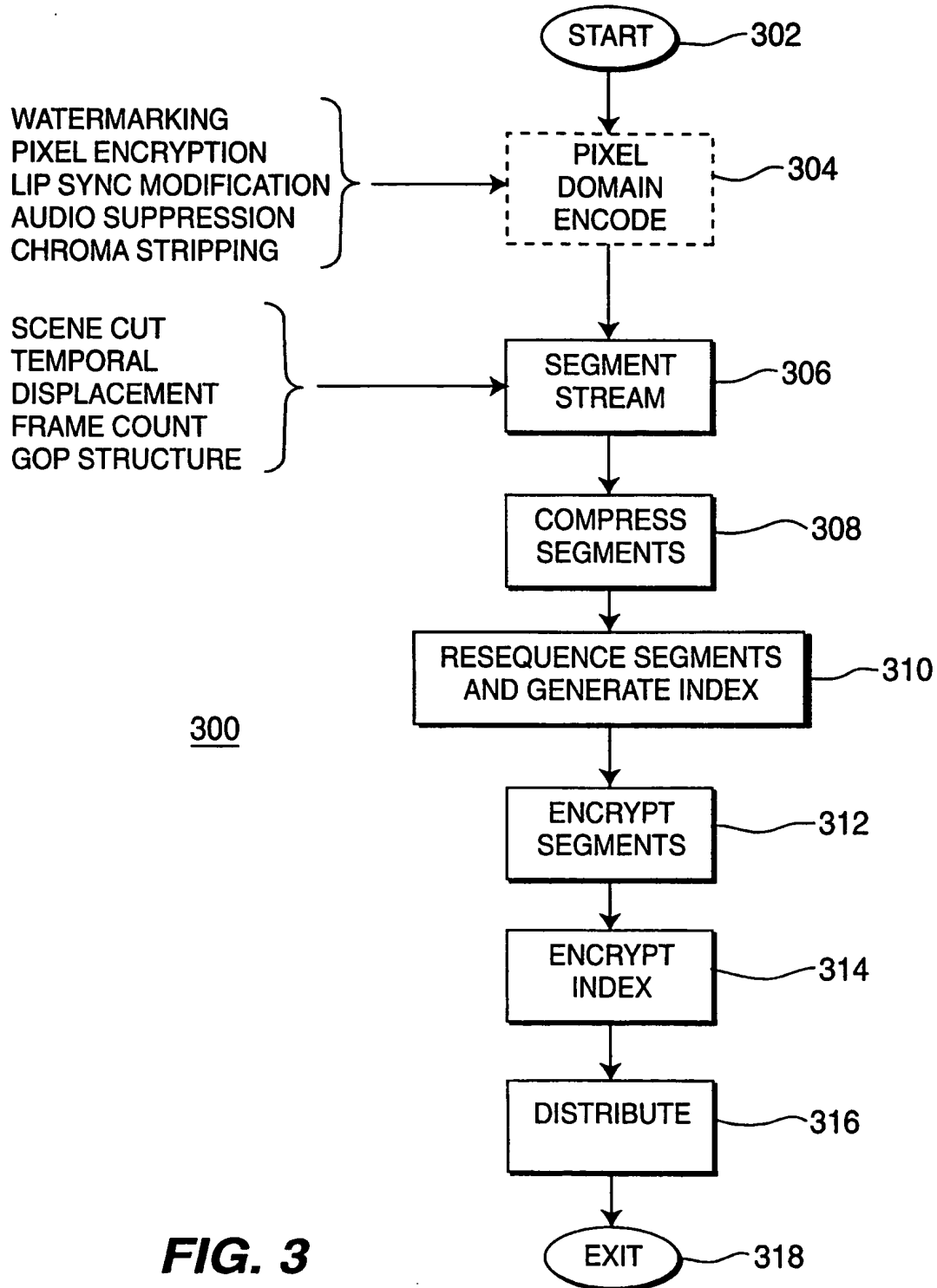
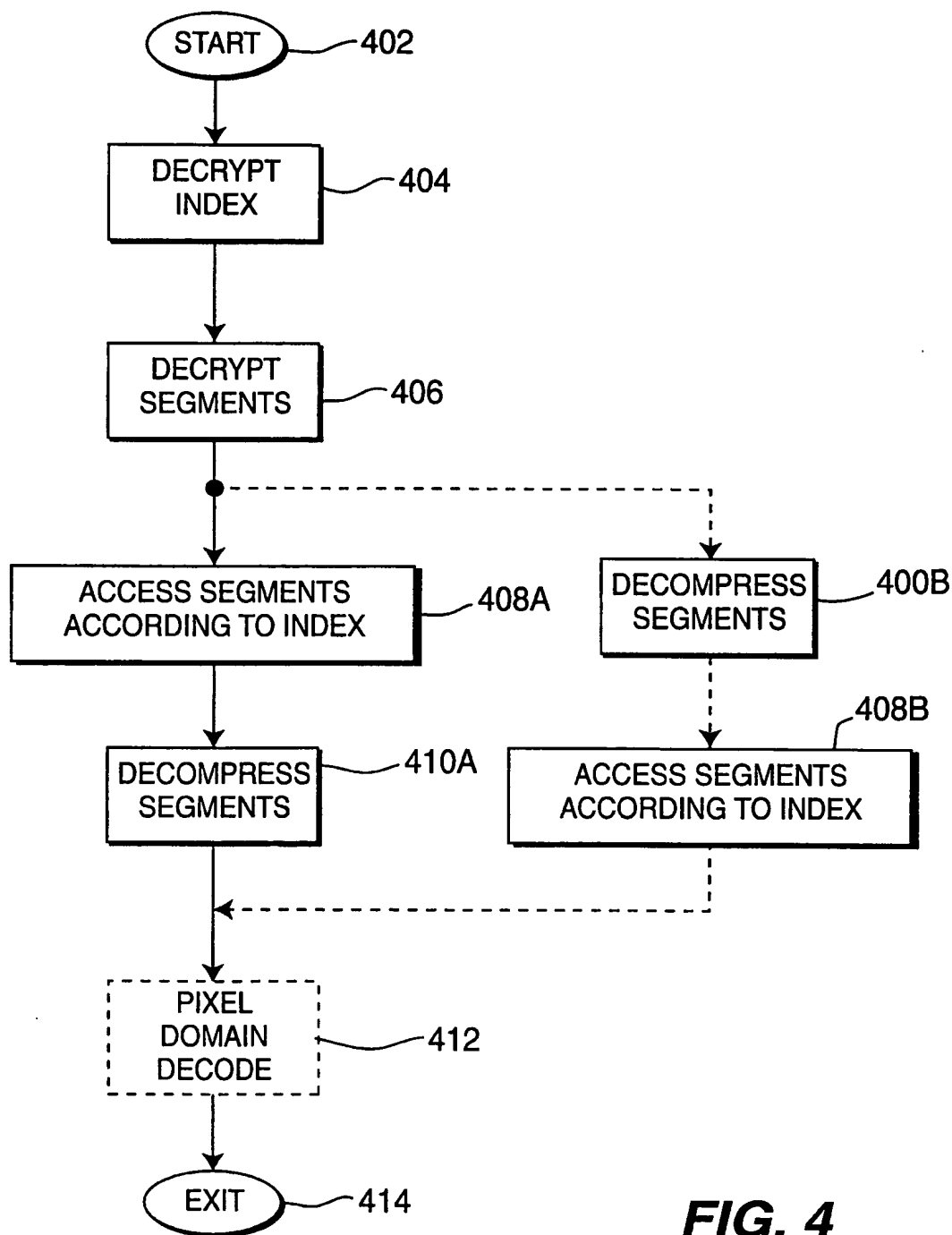


FIG. 2

3/5

**FIG. 3**

4/5

**FIG. 4**

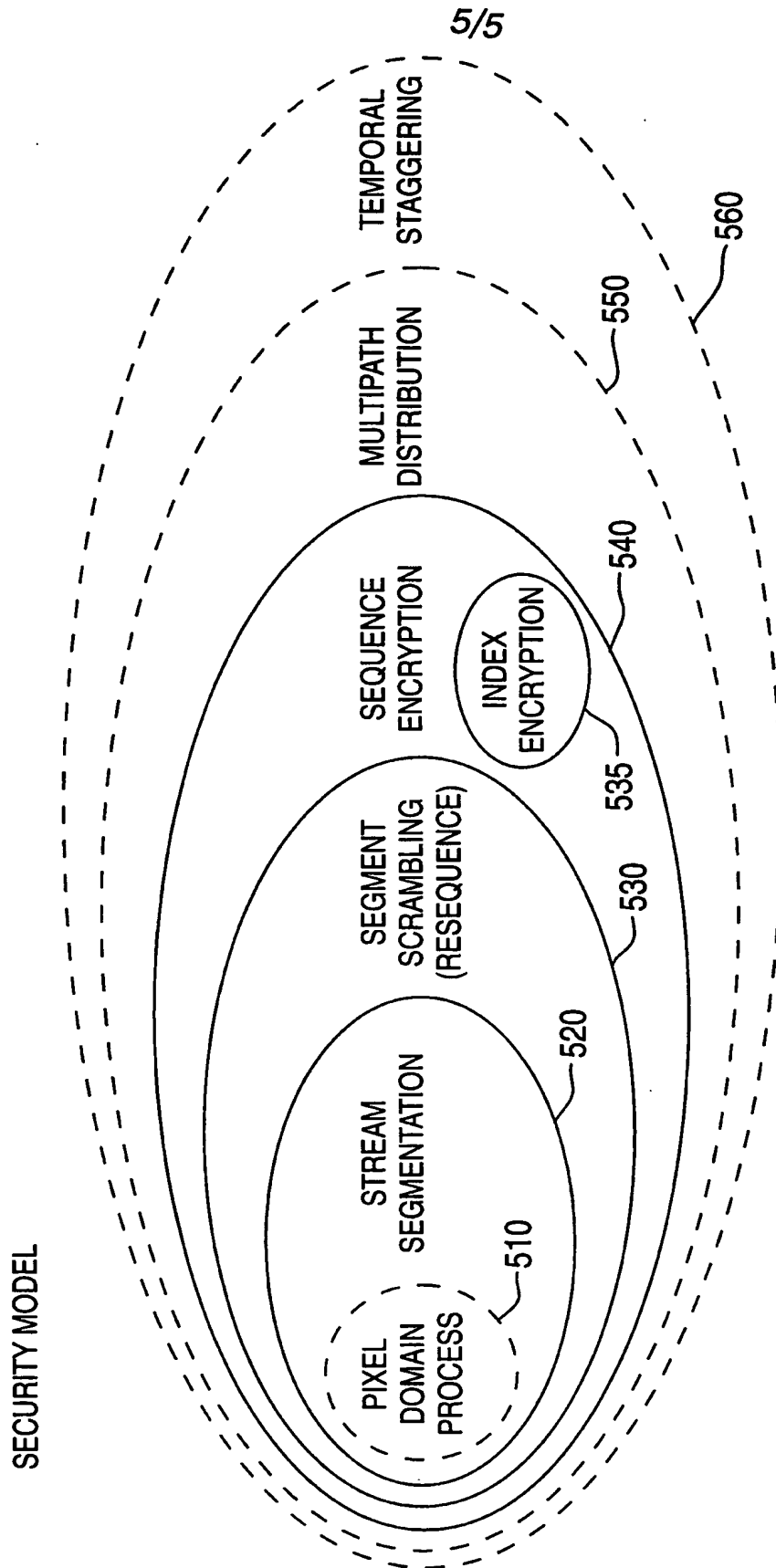


FIG. 5

INTERNATIONAL SEARCH REPORT

Inte. onal Application No

PCT/US 99/18417

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04N7/167 H04L9/06 H03M7/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N H04L H03M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 479 512 A (WEISS KENNETH P) 26 December 1995 (1995-12-26) column 6, line 27 -column 7, line 24 column 8, line 9 - line 19 ---	1, 10, 12
A	US 5 351 299 A (MATSUZAKI NATSUME ET AL) 27 September 1994 (1994-09-27) claim 18 ---	1, 10, 12
A	EP 0 710 025 A (SONY CORP) 1 May 1996 (1996-05-01) column 5, line 31 -column 6, line 23; figure 4 -----	1, 10, 12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 December 1999	12/01/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Augarde, E

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/18417

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5479512 A	26-12-1995	US 5657388 A	12-08-1997
		US 5485519 A	16-01-1996
		US 5367572 A	22-11-1994
		US 5237614 A	17-08-1993
		AU 681500 B	28-08-1997
		AU 1992495 A	03-10-1995
		CA 2183629 A	21-09-1995
		EP 0750814 A	02-01-1997
		JP 9510561 T	21-10-1997
		WO 9525391 A	21-09-1996
US 5351299 A	27-09-1994	JP 5344118 A	24-12-1993
		JP 6118872 A	28-04-1994
EP 0710025 A	01-05-1996	JP 8181689 A	12-07-1996
		US 5721778 A	24-02-1998